(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－311826
（P2002－311826A）
(43)公開日　平成14年10月25日(2002.10.25)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ	1/00	６１０Ａ　５Ｂ０３５
		６６０			６６０Ａ　５Ｊ０６４
Ｇ０６Ｋ	19/00		Ｈ０３Ｍ	7/30	Ｚ　５Ｊ１０４
	19/07		Ｇ０６Ｋ	19/00	Ｑ
Ｈ０３Ｍ	7/30				Ｎ

審査請求　未請求　請求項の数15　ＯＬ　（全 11 頁）

(21)出願番号　特願2001－116254(P2001－116254)

(22)出願日　平成13年４月16日(2001.4.16)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

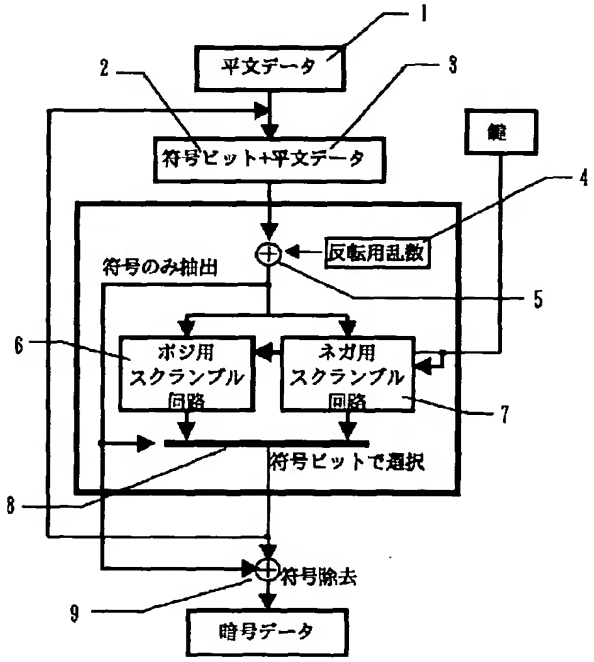
(71)出願人　000233169
株式会社日立超エル・エス・アイ・システムズ
東京都小平市上水本町５丁目22番１号

(74)代理人　100081938
弁理士　徳若　光政

最終頁に続く

(54)【発明の名称】　暗号化・復号化装置、暗号化・復号化方法、データの暗号化方法及びＩＣカード

(57)【要約】
【課題】　簡単な構成で安定的に機密保護の強化を実現した暗号化・復号化装置、暗号化・復号化方法及びＩＣカードを提供する。
【解決手段】　平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込み、かかるデータを上記非反転データに対応した転置・換字処理を行うポジ用スクランブル信号処理と、上記反転データに対応した転置・換字処理を行うネガ用スクランブル信号処理とを並列的に行ない、それぞれに対応した出力信号のいずれか一方を上記第１信号処理でのデータ選択動作に対応させて取り出す動作を複数回行なって最後の転置・換字の結果を暗号化データ又は復号化データとする。



1

【特許請求の範囲】

【請求項１】　平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込む入力選択回路と、

上記入力選択回路を通したデータを受け、上記非反転データに対応した転置・換字処理を行うポジ用スクランブル回路と、

上記入力選択回路を通したデータを受け、上記反転データに対応した転置・換字処理を行うネガ用スクランブル回路と、

上記ポジ用スクランブル回路又はネガ用スクランブル回路で転置・換字処理された出力信号のいずれか一方を上記入力選択回路の選択動作に対応させて取り出す出力選択回路と、

上記ポジ用スクランブル回路及びネガ用スクランブル回路での複数回の転置・換字の結果を最終転置する出力回路とを備え、

上記出力回路を通して暗号文又は平文データを得ることを特徴とする暗号化・復号化装置。

【請求項２】　請求項１において、

符号ビットを上記平文データ又は暗号文に対して付加する回路を更に含み、

ランダムに発生される選択信号を上記入力選択回路に供給して、上記符号ビットを含めて非反転データ又はその全ビットの反転データのいずれか一方を取り込むようにし、

上記符号ビットを分離して上記データを上記ポジ用スクランブル回路及びネガ用スクランブル回路で転置・換字処理し、

上記分離された符号ビットを用いて、上記出力選択回路を制御して入力選択回路で取り込まれた非反転データ又はその全ビットの反転データに対応した上記転置・換字処理された出力信号を取り出すことを特徴とする暗号化・復号化装置。

【請求項３】　請求項１又は２において、

上記転置・換字処理は、ＤＥＳ暗号・復号アルゴリズムにより行われるものであることを特徴とする暗号化・復号化装置。

【請求項４】　請求項２又は３において、

上記ランダムに発生される選択信号は、乱数発生回路で形成された１ビットの２値信号を受けて、その論理１と論理０の出現率をほぼ１／２に補正する補正回路で形成されることを特徴とする暗号化・復号化装置。

【請求項５】　平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込む第１信号処理と、

上記第１信号処理で取り込まれたデータを上記非反転データに対応した転置・換字処理を行うポジ用スクランブル信号処理と、上記反転データに対応した転置・換字処理を行うネガ用スクランブル信号処理とを並列的に行なう第２信号処理と、

2

上記ポジ用スクランブル信号処理又はネガ用スクランブル信号処理で転置・換字処理された出力信号のいずれか一方を上記第１信号処理でのデータ選択動作に対応させて取り出す第３信号処理と、

を複数回行ない、最後の転置・換字の結果を暗号化データ又は復号化データとしてなることを特徴とする暗号化・復号化方法。

【請求項６】　請求項５において、

上記平文データ又は暗号文に対して符号ビットを付加する動作と、

ランダムに発生される選択信号を形成する動作とを更に含み、

上記第１信号処理において、選択信号を用いて上記符号ビットを含めて非反転データ又はその全ビットの反転データのいずれか一方を取り込むようにし、

上記第２信号処理において、符号ビットを分離して上記ポジ用とネガ用のスクランブル信号処理を行ない、

上記第３信号処理において、上記分離された符号ビットを用いて上記第１信号処理において取り込まれた非反転データ又はその全ビットの反転データに対応した上記転置・換字処理された出力信号を取り出すようにしてなることを特徴とする暗号化・復号化方法。

【請求項７】　請求項５又は６において、

上記転置・換字処理をＤＥＳ暗号・復号アルゴリズムにより行うようにしてなることを特徴とする暗号化・復号化方法。

【請求項８】　請求項６又は７において、

上記ランダムに発生される選択信号は、乱数発生回路で形成された１ビットの２値信号の論理１と論理０の出現率をほぼ１／２に補正するような信号処理が行われることを特徴とする暗号化・復号化方法。

【請求項９】　入力されたデータに対し、所定の回数だけ所定の変換処理を行うことで、入力されたデータに対応した暗号化されたデータを得るデータの暗号化方法であって、

上記所定の変換処理は、論理０又は論理１のいずれかの状態をとる制御信号が入力され、入力データの全ビットを反転しない入力データについての処理を行ない第１のデータを生成し、入力データの全ビットを反転した入力データについての処理を行ない第２のデータを生成し、

上記制御信号の状態に応じて、上記第１データと上記第２データのいずれかを上記所定の変換処理の出力として出力し、

上記第１のデータの生成と上記第２データの生成とは並列的に行われ、

上記制御信号のとる状態は、論理０又は論理１のそれぞれの出現比率がおおよそ５０％となるように制御されていることを特徴とするデータの暗号化方法。

【請求項１０】　請求項９において、

上記制御信号のとる状態が、論理０又は論理１のそれぞれの出現比率がおおよそ５０％となるように制御するための制御装置を用いることを特徴とするデータの暗号化方法。

【請求項１１】　請求項１０において、

上記制御装置は、乱数発生装置を有することを特徴とするデータの暗号化方法。

【請求項１２】　外部端子がリードライト装置と電気的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含むＩＣカードであって、

上記暗号処理用演算ユニットは、

平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込む入力選択回路と、

上記入力選択回路を通したデータを受け、上記非反転データに対応した転置・換字処理を行うポジ用スクランブル回路と、

上記入力選択回路を通したデータを受け、上記反転データに対応した転置・換字処理を行うネガ用スクランブル回路と、

上記ポジ用スクランブル回路又はネガ用スクランブル回路で転置・換字処理された出力信号のいずれか一方を上記入力選択回路の選択動作に対応させて取り出す出力選択回路と、

上記ポジ用スクランブル回路及びネガ用スクランブル回路での複数回の転置・換字の結果を最終転置する出力回路とを備え、

上記出力回路を通して暗号文又は平文データを得るものであることを特徴とするＩＣカード。

【請求項１３】　請求項１２において、

符号ビットを上記平文データ又は暗号文に対して付加する回路を更に含み、

ランダムに発生される選択信号を上記入力選択回路に供給して、上記符号ビットを含めて非反転データ又はその全ビットの反転データのいずれか一方を取り込むようにし、

上記符号ビットを分離して上記データを上記ポジ用スクランブル回路及びネガ用スクランブル回路で転置・換字処理し、

上記分離された符号ビットを用いて、上記出力選択回路を制御して入力選択回路で取り込まれた非反転データ又はその全ビットの反転データに対応した上記転置・換字処理された出力信号を取り出すことを特徴とするＩＣカード。

【請求項１４】　請求項１２又は１３において、

上記転置・換字処理は、ＤＥＳ暗号・復号アルゴリズムにより行われるものであることを特徴とするＩＣカード。

【請求項１５】　請求項１３又は１４において、

上記ランダムに発生される選択信号は、乱数発生回路で形成された１ビットの２値信号を受けて、その論理１と論理０の出現率をほぼ１／２に補正する補正回路で形成されることを特徴とするＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、暗号化・復号化装置、暗号化・復号化方法、データの暗号化方法及びＩＣカードに関し、特にＩＣカードやプログラム内蔵の１チップマイクロコンピュータのようなＣＰＵとメモリを含み暗号鍵を使ったデータ処理を行なうものの機密保護技術に利用して有効な技術に関するものである。

【０００２】

【従来の技術】ＤＥＳ（Data Encryption Standard）は、広範に用いられている秘密鍵ブロック暗号である。ＤＥＳのアルゴリズムは、大きく平文のデータフローと鍵のデータフローに分割できる。平文データフローでは、ＩＰとよばれる転置（信号の入れ換え）を行った後、上位と下位それぞれ３２ビットずつにデータを分割し、転置・換字処理を１６回繰り返す。最後に上位と下位それぞれ３２ビットデータを統合し、IP^{-1}とよばれる転置を行い、暗号文を得る。ＤＥＳでは、暗号化と復号化が同じ処理で実現できる。ただし暗号化と復号化では、鍵のスケジューリングが異なる。鍵のスケジューリング部分について、詳細は省略するが、鍵データを元に、各段に対して４８ビット鍵スケジューリングデータの出力を行う。

【０００３】通常のＤＥＳアルゴリズムでは、同じ平文に対しては常に同じ内部動作を行う。その結果、内部信号が入力信号に依存して変化するので、ＤＰＡ(Diffrential Power Analysis)法での統計処理を行いやすい。つまり、ＤＰＡ法では、消費電流波形を統計処理して暗号鍵を推定し、例えばＤＥＳのある部分に仮定した暗号鍵を当てはめて、平文を変化させながら消費電流波形を測定して統計する。暗号鍵を様々に変化させながらこの作業を繰り返し、正しい鍵のときには電流波形が大きなピークを示す。

【０００４】上記のようなＤＰＡによるＤＥＳ解読に対する対策の例として、特開２０００－０６６５８５号公報がある。この公報に記載の技術では、マスクａのパターンと、そのビット反転のマスクパターンのペアを設け、暗号化を行う毎にこのペアの一方をスイッチによりランダムに選択して、装置内部の平文に依存したビットをマスクし、暗号文を出力する前に暗号文からマスクａの影響を除去するようにするものである。

【０００５】上記公報に記載の技術では、本来のデータにマスクし、各Ｓ箱に入力する直前でそのマスクを解除する。このマスクを解除したときにＤＰＡにより解読される恐れがあるので、Ｓ箱への入力直前におけるマスク

解除、マスク解除後の本来のデータによるＳ箱への入力、及びＳ箱からの出力のマスク操作を、事前に計算し、テーブルとして記憶し、テーブル参照することにより計算結果を求めるのでマスク解除のための排他的論理和の計算や、マスクをかけるための排他的論理和の計算が行われることはないのでＤＰＡによる解読を不可能にすることができる説明されている。

【０００６】

【発明が解決しようとする課題】しかしながら、上記公報の技術では、排他的論理和の計算を事前にテーブルとして記憶させる構成であり、上記マスクの機能を充分に発揮させるために本来のデータに相当するようなビットにする必要があり、その組み合わせも膨大になるので、かかる膨大な組み合わせからなるマスクに対応した演算結果を格納するテーブル（記憶回路）の回路規模が大きくなってしまう。また、ＤＰＡによる解読防止のためには、上記マスクが特定のパターンに偏らないようにする必要のあることは説明されているが、どのようにすれば複数ビットのパターンが偏らないようにできることの具体的な記述はなく、ＤＰＡによる解読の可能性を残している。

【０００７】この発明の目的は、簡単な構成で安定的に機密保護の強化を実現した暗号化・復号化装置、暗号化・復号化方法及びＩＣカードを提供することにある。この発明の前記ならびにそのほかの目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

【０００８】

【課題を解決するための手段】本願において開示される発明のうち代表的なものの概要を簡単に説明すれば、下記の通りである。すなわち、入力選択回路において、平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込み、かかる入力選択回路を通したデータを上記非反転データに対応した転置・換字処理を行うポジ用スクランブル回路及び反転データに対応した転置・換字処理を行うネガ用スクランブル回路に伝え、出力選択回路により上記ポジ用スクランブル回路又はネガ用スクランブル回路で転置・換字処理された出力信号のいずれか一方を上記入力選択回路の選択動作に対応させて取り出し、出力回路により上記ポジ用スクランブル回路及びネガ用スクランブル回路での複数回の転置・換字の結果を最終転置して暗号文又は平文データを得る。

【０００９】本願において開示される発明のうち他の代表的なものの概要を簡単に説明すれば、下記の通りである。すなわち、平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込み、かかるデータを上記非反転データに対応した転置・換字処理を行うポジ用スクランブル信号処理と、上記反転データに対応した

転置・換字処理を行うネガ用スクランブル信号処理とを並列的に行ない、それぞれに対応した出力信号のいずれか一方を上記第１信号処理でのデータ選択動作に対応させて取り出す動作を複数回行ない、最後の転置・換字の結果を暗号化データ又は復号化データとする。

【００１０】

【発明の実施の形態】図１には、この発明に係る暗号化・復号化装置、暗号化・復号化方法及びＩＣカードに適合されたＤＥＳ暗号コプロセッサの一実施例の概略ブロック図が示されている。この実施例では、ＤＥＳ暗号コプロセッサ内の平文信号（データ）１に１ビットからなる符号ビット２を付加して内部演算用信号３とする。上記符号ビットが”０”のとき、平文信号はポジ（信号値が平文値そのもの）を表す。符号ビットが”１”のときはネガ（信号値の反転値が平文値）を表す。平文信号および符号ビットは、演算ごとに反転用乱数信号４によって、排他的論理和５で内部演算信号全ビットを反転させる。

【００１１】スクランブル回路はポジ信号用６とネガ信号用７の２種類が別々に用意されており、符号ビット２の値により、ポジ信号用６とネガ信号用７の各出力信号をセレクタ８を用いて選択する。このような回路での１６回の繰り返し演算のあと、暗号データの出力の前に排他的論理和９を置き、符号ビット２が”１”なら暗号データを反転させる。

【００１２】図２には、本暗号コプロセッサが処理する暗号方式である、ＤＥＳ暗号のアルゴリズムを説明するための構成図が示されている。ＤＥＳの暗号化／復号化演算は、６４ビットの平文（暗号化の対象となるデータ）あるいは６４ビットの暗号文と、５６ビットの鍵を用いて行われる。

【００１３】ＤＥＳのアルゴリズムは、大きく平文のデータフローと鍵のデータフローに分割できる。平文データフローでは、ＩＰとよばれる初期転置（信号の入れ換え）を行った後、上位と下位それぞれ３２ビットずつにデータを分割し、図３で示された転置・換字処理を１６回繰り返す。最後に上位と下位それぞれ３２ビットデータを統合し、IP^{-1}とよばれる転置を行い、暗号文を得る。

【００１４】ＤＥＳでは、暗号化と復号化が同じ処理で実現できる。ただし暗号化と復号化では、鍵のスケジューリングが異なる。鍵のスケジューリング部分について、詳細は省略するが、鍵データを元に、各段に対して４８ビット鍵スケジューリングデータの出力を行う。

【００１５】図３に示された１６回の繰り返し演算部分は、転置処理、排他的論理和演算、およびＳＢＯＸとよばれる換字処理で構成されている。ＳＢＯＸは入力４８ビット、出力３２ビットの、変換テーブルを元にした換字処理である。ＳＢＯＸの変換テーブルは、ＦＩＰＳ－４６やＡＮＳＩ－８０、ＩＳＯでその内容が定義されて

いる。ＳＢＯＸの内部は、図４に示されているように、Ｓ１からＳ８の８つの換字処理部に分割される。それぞれの換字処理は、入力６ビット、出力４ビットである。

【００１６】上記のようなＤＥＳアルゴリズムをそのままハードウェア化した際に問題点となるのは、ＤＰＡ(Differential Power Analysis)による電流解析に弱い点である。ＤＰＡアタックは、チップの消費電流波形から暗号鍵の値を推定する解析手法である。ＤＰＡでは、アタッカーはまずチップに平文データを与え、そのデータを処理する際の消費電流波形を計測する。次に、チップ内部に納められた秘密鍵の値（の一部）を仮定し、着目した信号線の変化(=消費電流の微小増加）の予測を、実際の消費電流波形に適用する。仮定した鍵が正しい場合、消費電流の増加が増幅され、ピークとなって表れる。ＤＥＳ暗号は元々、ハードウェア化が容易になるよう設計されたアルゴリズムである。そのためＤＥＳ暗号処理用のハードウェアを設計すると、どの製品でも似たような内部構造となる。これがＤＰＡによる解析を容易にしている。

【００１７】ＤＰＡによる解析を困難にする方法として、前記のように特開２０００－０６６５８５号公報のように、演算ごとに内部データや処理内容を変化させるという方法がある。内部データを毎回変える方法で簡単なのは、平文に何らかのスクランブル用コードとの排他的論理和をかける方法である。しかしこの方法だと、転置処理を行う度に、データにかかっているスクランブルコードの値が変わる。そのため、演算データにかかっているスクランブルコードの値を保持しておく必要がある。

【００１８】この発明では、演算データの全ビットを反転させるか否かをランダムに決定する方式をとる。この方式だと、演算データに１ビットの符号データを付与するだけで、現在の演算データの状態（反転／非反転）を保持できる。また、転置と排他的論理和の影響を受けない。ただし、ＳＢＯＸだけは反転データと非反転データで変換テーブルが異なるため、非反転データ用（通常のＳＢＯＸ）と、本願によって追加された反転データ用（ＳＢＯＸ－ＢＡＲ）の二種類のＳＢＯＸが用意される。そして符号ビットにより、ＳＢＯＸとＳＢＯＸ－ＢＡＲのどちらを使用するかを選択する。つまり、２つのＳＢＯＸとＳＢＯＸ－ＢＡＲのいずれか一方の出力信号を有効として取り出す。

【００１９】上記ＳＢＯＸの作り方を、Ｓ１を例に説明すると次の通りである。ＤＥＳ規格に基づくＳ１の換字構成を図５に示す。図５（ａ）の横方向が入力６ビット中４ビットで表される数字（０～１５）、縦方向が入力の残り２ビット（０～３）、書かれている数字がその入力に対する出力４ビット（０～１５）を表している。反転データ用Ｓ１－ＢＡＲは、図６（ｂ）に示すように、論理的にはＳ１の入力と出力両方を反転させることで作成する。図５（ｂ）にＳ１－ＢＡＲの換字構成が示されている。図５（ａ）左上の”１４”は、入力が”００００００”のときの出力値を表している。この出力に対応するＳ１－ＢＡＲは、図５（ｂ）の右下（入力”１１１１１１”に相当）の、”１４”を反転させた”１”にあたる。

【００２０】実際のコプロセッサに組み込むのは、図５（ｂ）のように再計算した換字構成である。すなわち、図６（ａ）の非反転データ用に対応したＳＢＯＸに対して、図６（ｂ）に示したように、同じＳＢＯＸに対して入力と出力にインバータ回路を設けたような論理をそのまま使用するわけではない。

【００２１】本発明の変形例としては、図７（ａ）示したように入力側のみにインバータ回路を設けたＳＢＯＸ、あるいは図７（ｂ）に示したように出力側にのみインバータ回路を設けたＳＢＯＸと等価な換字構成（表）を用いたＳＢＯＸのペアを使用することも可能である。

【００２２】図８には、本発明に係る暗号化・復号化装置、暗号化・復号化方法を説明するための基本構造（平文の転置・換字処理部分）の一実施例のブロック図が示されている。ＩＰ、ＩＰ-1、鍵スケジューリング部は、前記図２ないし図４を用いて説明したＤＥＳの基本アルゴリズムと同じなので、その説明を省略する。図８において、Ａで表される個所が図１において演算データを反転か否かをランダムに決定する部分、Ｂで表される個所が２つのＳＢＯＸの出力を選択する部分である。

【００２３】図８において、Ａの部分をインバータ回路を通した反転信号と、その入力信号とを選択信号で制御されるマルチプレクサで出力させるように示されているが、図９で示したように、１ビットの選択信号を共通に受ける排他的論理和を使用しても等価な回路が構成できる。つまり、符号ビットを含んだ３３ビットの入力データは、選択信号が論理０ならそのまま出力され、選択信号が論理１なら上記３３ビットの入力信号が反転されて出力される。図８のようにインバータ回路とマルチプレクサを用いた場合でも、図９のように排他的論理和回路を用いた場合でも、ＭＯＳＦＥＴで構成した場合には基本的にはほぼ同じ回路素子で構成できるのでいずれを選んでも大差はない。

【００２４】図１０には、演算データ反転部分のデータフローを説明するためのブロック図が示されている。図１０（ａ）は、選択信号、つまりデータの反転／非反転を決定する乱数信号の値が”０”のときの動作を示している。図１０（ｂ）は、選択信号が”１”のときの動作を示している。前段から来るデータをＭとすると、選択信号が”０”のときには、図１０（ａ）のように、拡大転置Ｅに入るデータはＭが選択される。選択信号が”１”のときには、図１０（ｂ）のように、拡大転置Ｅに入るデータとしてＭＢ（Ｂは図１０（ｂ）の反転信号であるバーを表している）が選択される。拡大転置Ｅの出

力はそれぞれＥ（Ｍ）、Ｅ（ＭＢ）となる。拡大転置Ｅは信号の並び換え処理なので、Ｅ（ＭＢ）はＥ（Ｍ）Ｂと等しい。結局、Ｍに対する拡大転置Ｅの出力は、選択信号＝”０”のときにＥ（Ｍ）、選択信号＝”１”のときにＥ（Ｍ）の反転値となる。

【００２５】図１１には、ＳＢＯＸ出力選択部分のデータフローを説明するためのブロック図が示されている。出力の選択は、ＳＢＯＸに入るデータの符号ビットによって行われる。図１１（ａ）に示すように、ＳＢＯＸに入力されるデータがＸ（符号信号＝”０”）の場合、非反転データ用のＳＢＯＸの出力が選択される。図１１（ｂ）に示すように、入力信号がＸＢ（Ｘの反転データ、符号信号＝”１”）の場合、反転データ用のＳＢＯＸ－ＢＡＲの出力が選択される。

【００２６】図１２には、データの反転／非反転用の選択信号を形成する回路の一実施例のブロック図が示されている。この実施例では、選択信号として、ＩＣカードに搭載されている乱数発生器の非同期発振信号を使用している。ただし非同期発振信号は温度や電圧によって出力に偏りがでるため、補正回路を介してから使用している。補正回路により、非同期発振信号が０あるいは１にスタックした場合でも、０／１の比率が５０％に近い信号を選択信号として使用することができる。

【００２７】図１３には、この発明に用いられる０／１比率補正回路の一実施例のブロック図が示されている。この実施例では、８段のシフトレジスタがリング状に接続される。シフトレジスタの初段回路Ｂ１には、その出力信号と最終段Ｂ８の出力信号との排他的論理和が採られて入力信号とされる。第２段目Ｂ２の出力信号は、乱数発生器より供給される非同期発振信号の出力と排他的論理和が採られて第３段目Ｂ３の入力信号とされる。以下、第３段目Ｂ３から最終段Ｂ８までは順次に伝えられる。そして、特に制限されないが、第６段目Ｂ６の出力信号が選択信号として用いられる。

【００２８】この実施例では、シフトレジスタＢ２～Ｂ８で記憶されたビットが連続して同じ値になったときに、Ｂ１での排他的論理和処理により適宜反転させ、かつ乱数発生器からの非同期発振信号が連続して、論理０又は１に偏った場合にも、シフト段Ｂ２とＢ３の間で適宜に反転させて、論理０と論理１の出現率を５０％ずつに補正するものである。

【００２９】本発明において、耐ＤＰＡ強度を決定するのが、反転／非反転用の選択信号である。チップ内部信号の０／１出現比率を５０％に近くすることで、ＤＰＡによる解析を困難にすることが可能となる。つまり、前記のようにＤＰＡでは、データを処理する際の消費電流波形を計測して統計的手法によってピークを探すので、上記０／１出現比率を５０％にすることにより、統計処理での消費電流が平均化されてピークが無くなってしまうので、かかるＤＰＡによる解読が困難になるものである。

【００３０】この実施例では、前記説明したように、平文データに符号ビットを付加し、ポジ／ネガの両方の状態を持つようにする。暗号化における繰り返し演算時に、データを符号ごとランダムに変更する。符号の影響を受けない演算（排他的論理和など）はそのまま符号を無視して演算する。符号の影響を受ける演算（変換表を用いた演算など）では、ポジ用の演算回路とネガ用の演算回路を用意し、データの符号によって演算回路の出力を選択する機構を用いる。

【００３１】この実施例に従えば、暗号演算時間が増加しない。例えばダミーの演算を行うなど、演算時間を延ばして撹乱する方法もあるが、本方法は演算するたびに内部処理内容が異なるという撹乱方法をとっているため、１回の演算にかかる時間は未対策のときと同じである。そして、この実施例では、ＤＰＡ対策をハードウェアに盛り込んでいるので、ソフトウェアにより対策を採る場合のようにユーザに余分な負荷をかけない。

【００３２】図１４には、この発明が適用されるＩＣカードの一実施例の外観図が示されている。ＩＣカードは、プラスチックケースからなるカード１０１と、かかるカード１０１の内部に搭載された図示しない１チップのマイクロコンピュータ等からなるＩＣカード用チップを持つものである。上記ＩＣカードは、さらに上記ＩＣカード用チップの外部端子に接続されている複数の接点（電極）１０２を持つ。複数の接点１０２は、後で図１５によって説明するような電源端子ＶＣＣ、電源基準電位端子ＶＳＳ、リセット入力端子ＲＥＳバー、クロック端子ＣＬＫ、データ端子Ｉ／Ｏ－１／ＩＲＱバー、Ｉ／Ｏ－２／ＩＲＱバーとされる。ＩＣカードは、かかる接点１０２を通して図示しないリーダーライタのような外部結合装置から電源供給を受け、また外部結合装置との間でのデータの通信を行う。

【００３３】図１５には、この発明に係るＩＣカードに搭載されるＩＣカード用チップ（マイクロコンピュータ）の一実施例の概略ブロック図が示されている。同図の各回路ブロックは、公知のＭＯＳ集積回路の製造技術により、特に制限されないが、単結晶シリコンのような１個の半導体基板上において形成される。

【００３４】この発明に係るＩＣカード用チップの構成は、基本的にマイクロコンピュータと同じような構成である。その構成は、クロック生成回路、中央処理装置（以下、単にＣＰＵという）、ＲＯＭ(Read Only Memory)やＲＡＭ(Random Access Memory)、不揮発性メモリ（ＥＥＰＲＯＭ）などの記憶装置、暗号化及び復号化処理の演算を行なうコプロセッサ（暗号化・復号化装置）、入出力ポート（Ｉ／Ｏポート）などからなる。

【００３５】クロック生成回路は、図示しないリーダライタ（外部結合装置）から図１の接点１０２を介して供給される外部クロックＣＬＫを受け、かかる外部クロッ

ク信号に同期したシステムクロック信号を形成し、それをチップ内部に供給する回路である。ＣＰＵ２０１は、論理演算や算術演算などを行う装置であり、システムコントロールロジック、乱数発生器及びセキュリィロジック及びタイマなどを制御する。ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭのような記憶装置は、プログラムやデータを格納する装置である。コプロセッサは、前記説明したようりＤＥＳ暗号法などに適合された回路から構成される。Ｉ／Ｏ（入出力）ポートは、リーダライタと通信を行う装置である。データバスとアドレスバスは、各装置を相互に接続するバスである。

【００３６】上記記憶装置のうち、ＲＯＭは、記憶内容が不揮発的に固定されているメモリであり、主にプログラムを格納するメモリである。揮発性メモリ（以下、ＲＡＭという）は自由に記憶情報の書き換えができるメモリであるが、電源の供給が中断されると、記憶している内容が消えてなくなる。ＩＣカードがリーダライタから抜かれると電源の供給が中断されるため、上記ＲＡＭの内容は、保持されなくなる。

【００３７】上記不揮発性メモリ（以下、ＥＥＰＲＯＭ (Electrical Erasable Programmable Read Only Memory）という）は、内容の書き換えが可能な不揮発性メモリであり、その中に一旦書き込まれた情報は、電源の供給が停止されてもその内部に保持される。このＥＥＰＲＯＭは、書き換える必要があり、かつＩＣカードがリーダライタから抜かれても保持すべきデータを格納するために使われる。例えば、ＩＣカードがプリペイドカードとして使用されるような場合、のプリペイドの度数などは、使用するたびに書き換えられる。この場合の度数などは、リーダライタか抜かれてもＩＣカード内で記憶保持する必要があるため、ＥＥＰＲＯＭで保持される。

【００３８】ＣＰＵは、いわゆるマイクロプロセッサと同様な構成にされる。すなわち、その詳細を図示しないけれども、その内部に命令レジスタ、命令レジスタに書込まれた命令をデコードし、各種のマイクロ命令ないしは制御信号を形成するマイクロ命令ＲＯＭ、演算回路、汎用レジスタ（ＲＧ６等）、内部バスＢＵＳに結合するバスドライバ、バスレシーバなどの入出力回路を持つ。ＣＰＵは、ＲＯＭなどに格納されている命令を読み出し、その命令に対応する動作を行う。ＣＰＵは、Ｉ／Ｏポートを介して入力される外部データの取り込み、ＲＯＭからの命令や命令実行のために必要となる固定データのようなデータの読み出し、ＲＡＭやＥＥＰＲＯＭに対するデータの書き込みと読み出し動作制御等を行う。

【００３９】上記ＣＰＵは、クロック生成回路から発生されるシステムクロック信号を受けそのシステムクロック信号によって決められる動作タイミング、周期をもって動作される。ＣＰＵは、その内部の主要部がＰチャンネル型ＭＯＳＦＥＴとＮチャンネル型ＭＯＳＦＥＴとからなるＣＭＯＳ回路から構成される。特に制限されない

が、ＣＰＵは、ＣＭＯＳスタティックフリップフロップのようなスタティック動作可能なＣＭＯＳスタテック回路と、信号出力ノードへの電荷のプリチャージと信号出力ノードへの信号出力とをシステムクロック信号に同期して行うようなＣＭＯＳダイナミック回路とを含む。

【００４０】コプロセッサは、前記説明したように内部で扱う平文データに符号ビットを付加し、ポジ／ネガの両方の状態を持つようにする。暗号化における繰り返し演算時に、データを符号ごとランダムに変更する。符号の影響を受けない演算（排他的論理和など）はそのまま符号を無視して演算する。符号の影響を受ける演算（変換表を用いた演算など）では、ポジ用の演算回路とネガ用の演算回路を用意し、データの符号によって演算回路の出力を選択する機構を用いる。

【００４１】この実施例のＩＣカードにおいても、演算するたびに内部処理内容が異なるという撹乱方法をとっているため、１回の演算にかかる時間は未対策のときと同じであるので、高速なデータ処理が可能であり、ＤＰＡ対策をハードウェアに盛り込んでいるので、ＤＰＡ対策のためにＣＰＵが余分な動作を行う必要がないのでユーザに余分な負荷をかけなくて済む。

【００４２】上記の実施例から得られる作用効果は、下記の通りである。すなわち、

（１）　入力選択回路において、平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込み、かかる入力選択回路を通したデータを上記非反転データに対応した転置・換字処理を行うポジ用スクランブル回路及び反転データに対応した転置・換字処理を行うネガ用スクランブル回路に伝え、出力選択回路により上記ポジ用スクランブル回路又はネガ用スクランブル回路で転置・換字処理された出力信号のいずれか一方を上記入力選択回路の選択動作に対応させて取り出し、出力回路により上記ポジ用スクランブル回路及びネガ用スクランブル回路での複数回の転置・換字の結果を最終転置して暗号文又は平文データを得ることにより、簡単な構成で高速にしかも安定的にＤＰＡ対策による機密保護を実現できるという効果が得られる。

【００４３】（２）　上記に加えて、符号ビットを上記平文データ又は暗号文に対して付加し、ランダムに発生される選択信号を上記入力選択回路に供給して、上記符号ビットを含めて非反転データ又はその全ビットの反転データのいずれか一方を取り込むようにし、上記符号ビットを分離して上記データを上記ポジ用スクランブル回路及びネガ用スクランブル回路で転置・換字処理し、分離された上記符号ビットを用いて、上記出力選択回路を制御して入力選択回路で取り込まれた非反転データ又はその全ビットの反転データに対応した上記転置・換字処理された出力信号を取り出すことにより、簡単な構成によりＤＰＡ対策を実現できるという効果が得られる。

13

【００４４】（３）　上記に加えて、上記転置・換字処理をＤＥＳ暗号・復号アルゴリズムにより行うようにすることにより、暗号化と復号化が同じ処理で実現できるから回路の簡素化が可能になるという効果が得られる。

【００４５】（４）　上記に加えて、ランダムに発生される選択信号を、乱数発生回路で形成された１ビットの２値信号を受けて、その論理１と論理０の出現率をほぼ１／２に補正するという簡単な回路を付加することにより、より強固なＤＰＡ対策を実現できるという効果が得られる。

【００４６】以上本発明者よりなされた発明を実施例に基づき具体的に説明したが、本願発明は前記実施例に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。例えば、ＩＣカードには、１つの半導体集積回路装置を搭載するもの他、複数の半導体集積回路装置が搭載されるものであってもよい。暗号化・復号化装置が搭載されるマイクロコンピュータは、１つの半導体集積回路装置に形成されるもの他、ＣＰＵとその周辺回路が複数チップで構成されて、１つのモジュール基板に搭載されてなるものであってもよい。

【００４７】上記マイクロコンピュータは、データ処理装置とかかるデータ処理装置によるデータ処理手順が書き込まれたＲＯＭを含んで上記データ処理手順に従ってデータの入出力動作が行われるものであれば何であってもよい。例えば、前記のようなＩＣカード用チップの他に、ゲーム用等の１チップマイクロコンピュータ等のように機密保護の必要な各種マイクロコンピュータに広く適用できるものである。この発明は、暗号化・復号化装置、暗号化・復号化方法、データの暗号化方法及び機密保護を必要とする各種ＩＣカードやマイクロコンピュータに広く利用できる。

【００４８】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば、下記の通りである。すなわち、入力選択回路において、平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込み、かかる入力選択回路を通したデータを上記非反転データに対応した転置・換字処理を行うポジ用スクランブル回路及び反転データに対応した転置・換字処理を行うネガ用スクランブル回路に伝え、出力選択回路により上記ポジ用スクランブル回路又はネガ用スクランブル回路で転置・換字処理された出力信号のいずれか一方を上記入力選択回路の選択動作に対応させて取り出し、出力回路により上記ポジ用スクランブル回路及びネガ用スクランブル回路での複数回の転置・換字の結果を最終転置して暗号文又は平文データを得ることにより、簡単な構成で高速にしかも安定的にＤＰＡ対策による機密保護を実現できる。

14

【図面の簡単な説明】

【図１】この発明に係る暗号化・復号化装置、暗号化・復号化方法及びＩＣカードに適合されたＤＥＳ暗号コプロセッサの一実施例を示す概略ブロック図である。

【図２】この発明に用いられるＤＥＳ暗号のアルゴリズムを説明するための構成図である。

【図３】この発明に用いられるＤＥＳ暗号のアルゴリズムにおける演算部分を説明するためのブロック図である。

【図４】この発明に用いられるＤＥＳ暗号のアルゴリズムにおけるＳＢＯＸの内部を説明するための構成図である。

【図５】この発明に用いられるＤＥＳ暗号のアルゴリズムにおけるＳＢＯＸの作り方を、Ｓ１を例にした説明図である。

【図６】この発明に係るＳＢＯＸの作り方を、Ｓ１を例にして論理的に説明するための説明図である。

【図７】この発明に係るＳＢＯＸの作り方の他の一例をを、Ｓ１を例にして論理的に説明するための説明図である。

【図８】本発明に係る暗号化・復号化装置、暗号化・復号化方法を説明するための基本構造（平文の転置・換字処理部分）の一実施例を示すブロック図である。

【図９】本発明に係る暗号化・復号化装置、暗号化・復号化方法における入力選択回路の他の一実施例を説明するためのブロック図である。

【図１０】本発明に係る暗号化・復号化装置、暗号化・復号化方法における演算データ反転部分のデータフローを説明するためのブロック図である。

【図１１】本発明に係る暗号化・復号化装置、暗号化・復号化方法におけるＳＢＯＸ出力選択部分のデータフローを説明するためのブロック図である。

【図１２】本発明に係る暗号化・復号化装置、暗号化・復号化方法におけるデータの反転／非反転用の選択信号を形成する回路の一実施例を示すブロック図である。

【図１３】この発明に用いられる０／１比率補正回路の一実施例を示すブロック図である。

【図１４】本発明に係るＩＣカードの一実施例を示す外観図である。

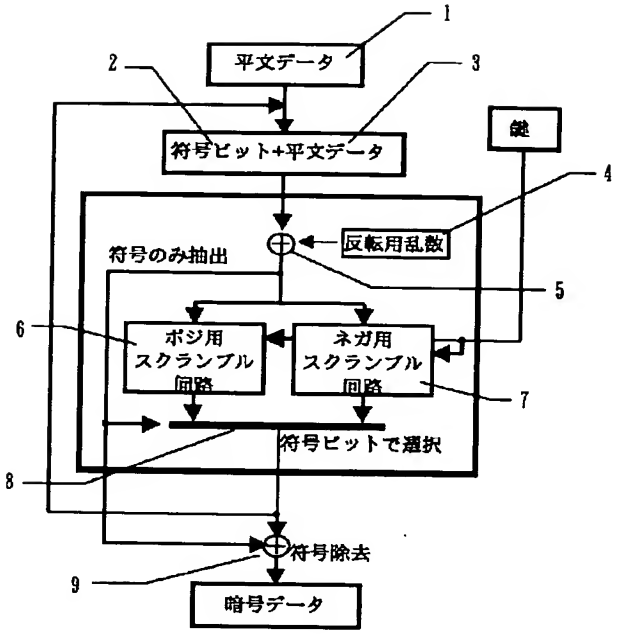
【図１５】本発明に係るＩＣカードに搭載されるＩＣカード用チップ（マイクロコンピュータ）の一実施例を示す概略ブロック図である。

【符号の説明】

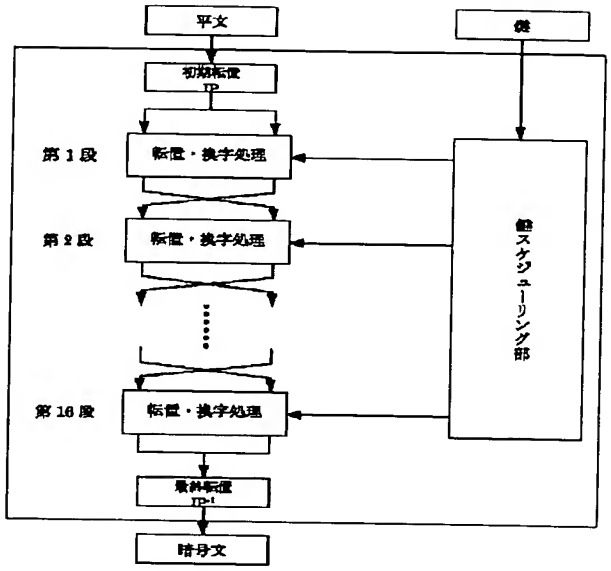
１…平分信号、２…符号ビット、３…内部演算用信号、４…反転用乱数信号、５…排他的論理和、６…ポジ用スクランブル回路、７…ネガ用スクランブル回路、８…セレクタ、９…排他的論理和、１０１…カード、１０２…接点

ＲＡＭ・ランダム・アクセス・メモリ、ＲＯＭ…リード・オンリ・メモリ、ＥＥＰＲＯＭ…不揮発性メモリ、

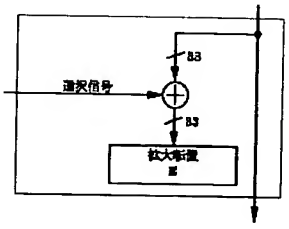
【図１】



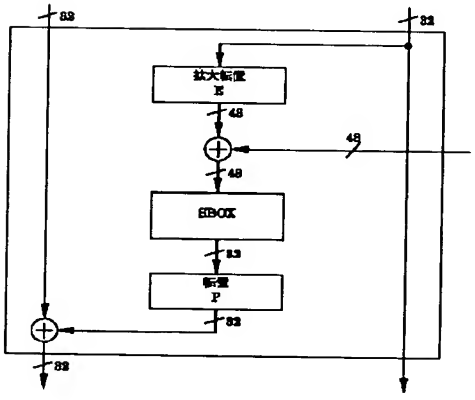
【図２】



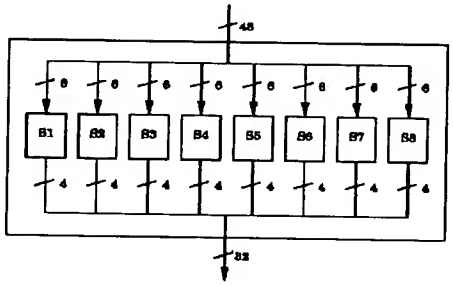
【図９】



【図３】



【図４】



【図５】

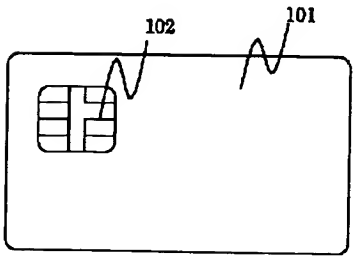
（ａ）Ｓボックス(S1)の換字表

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	5
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

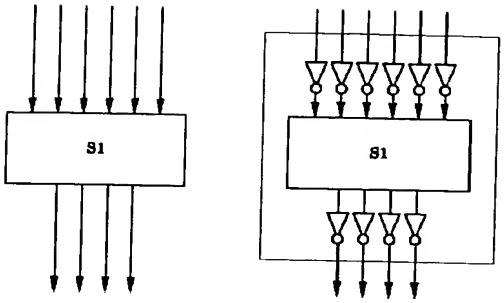
（ｂ）Ｓボックス BAR(S1-BAR)の換字表

2	9	15	5	1	12	4	10	8	14	6	11	13	7	3	0
15	10	5	12	8	6	3	0	4	13	9	2	7	1	14	11
7	12	10	6	4	3	9	5	14	2	13	1	11	8	0	15
8	15	6	10	3	9	5	12	7	4	0	13	14	2	11	1

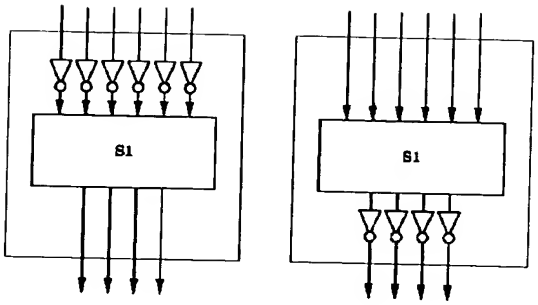
【図１４】



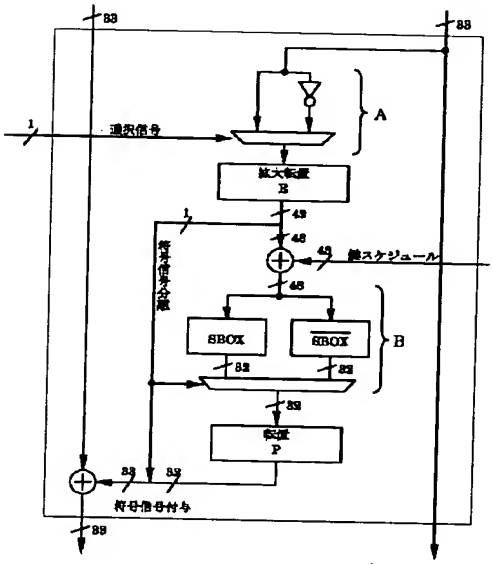
【図６】



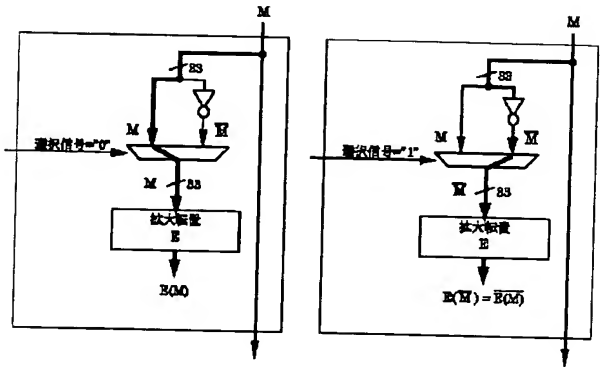
【図７】



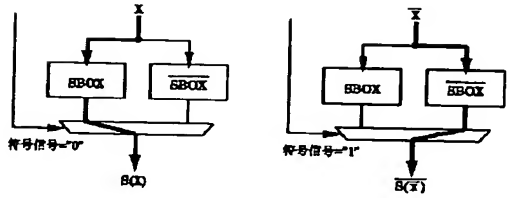
【図８】



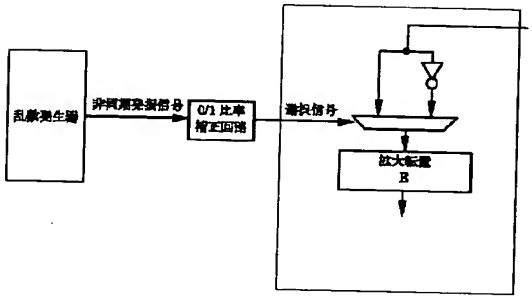
【図１０】



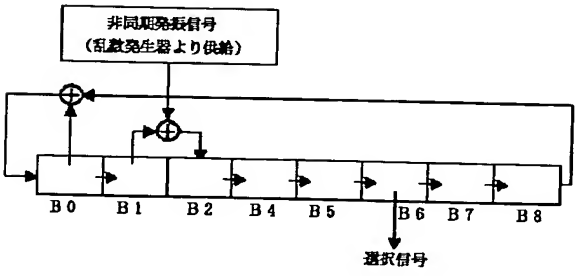
【図１１】



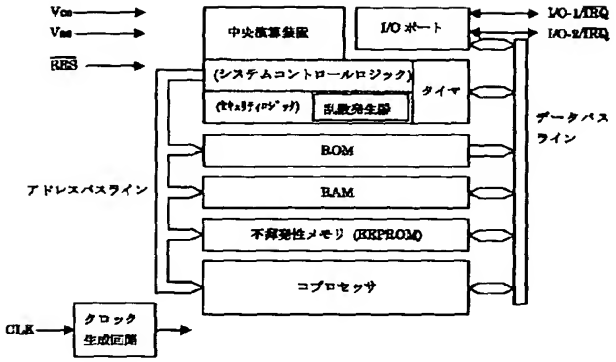
【図１２】



【図１３】



【図１５】



フロントページの続き

(72) 発明者　▲高▼橋　雅聡
東京都小平市上水本町５丁目22番１号　株式会社日立超エル・エス・アイ・システムズ内

Ｆターム(参考)　5B035 AA13 BB09 BC02 CA38
5J064 AA04 BC01 BC02 BC03 BD02 BD03
5J104 AA47 JA03 JA13 NA02